ABSTRACT

Elliptical curve based cryptographic algorithms are public key algorithms offering a shorter calculation time and smaller key sizes in comparison with RSA. In a smart card type environment, these algorithms are vulnerable to differential power analysis (DPA) attacks. The disclosed invention provides a countermeasure procedure enabling positive action to be taken against DPA-type attacks. The countermeasure does not reduce performance and is easy to use in a smartcard type component